2017

Biometric encryption system for increased security

Ranjith Jayapal
University of North Florida, n01054475@unf.edu

BIOMETRIC ENCRYPTION SYSTEM FOR INCREASED SECURITY

by

Ranjith Jayapal

A thesis submitted to the College of Computing, Engineering & Construction in partial fulfillment of the requirements for the degree of

Master of Science in Electrical Engineering

UNIVERSITY OF NORTH FLORIDA

COLLEGE OF COMPUTING, ENGINEERING & CONSTRUCTION

April 2017

This thesis titled “Biometric Encryption System for Increased Security” by Ranjith Jayapal is approved by:

Date

_____ _____

Dr. Pramod Govindan, Advisor

_____ _____

Dr. O Patrick Kreidl, Committee Member

_____ _____

Dr. Swapnoneel Roy, Committee Member

Accepted for the School of Engineering:

_____ _____

Director of the School of Engineering

Dr. Murat Tiryakioglu, CQE

Accepted for the College of Computing, Engineering and Construction:

_____ _____

Dr. Mark A. Tumeo, PE

Dean of the College of Computing, Engineering and Construction

Accepted for the University:

_____ _____

Dr. John Kantner

Dean of the Graduate School

ACKNOWLEDGEMENTS

I would like to thank the thesis committee members, Dr. Pramod Govindan, my supervising professor, for his continuous guidance and encouragement during the course of my thesis; Dr. O Patrick Kreidl and Dr. Swapnoneel Roy for their feedback and advice. I offer my sincere appreciation for all the support and learning opportunities provided by the committee members. Additionally, I thank Michael Bourg, for reviewing my thesis and helping to improve my English proficiency.

Furthermore, I thank the University of North Florida, College of Computing, Engineering & Construction and the Graduate School staff & faculty members for supporting me on my journey to successfully complete the master's program.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

ABSTRACT

Security is very important in present day life. In this highly-interconnected world, most of our daily activities are computer based, and the data transactions are protected by passwords. These passwords identify various entities such as bank accounts, mobile phones, etc. [10]. People might reuse the same password, or passwords related to an individual that can lead to attacks [20]. Indeed, remembering several passwords can become a tedious task. Biometrics is a science that measures an individual's physical characteristics in a unique way. Thus, biometrics serves as a method to replace the cumbersome use of complex passwords. Our research uses the features of biometrics to efficiently implement a biometric encryption system with a high level of security.

CHAPTER 1: BIOMETRIC ENCRYPTION OVERVIEW

By using a Biometric Encryption (BE) method, one can personalize the biometric to encode a PIN, a password, or an alphanumeric string, for a multitude of applications such as, bank ATMs, building access, and computer terminal access. Basically, no PIN numbers to be remembered in this case [20]. Moreover, the database only needs to store the biometrically encrypted PIN or password, not the large biometric sample.

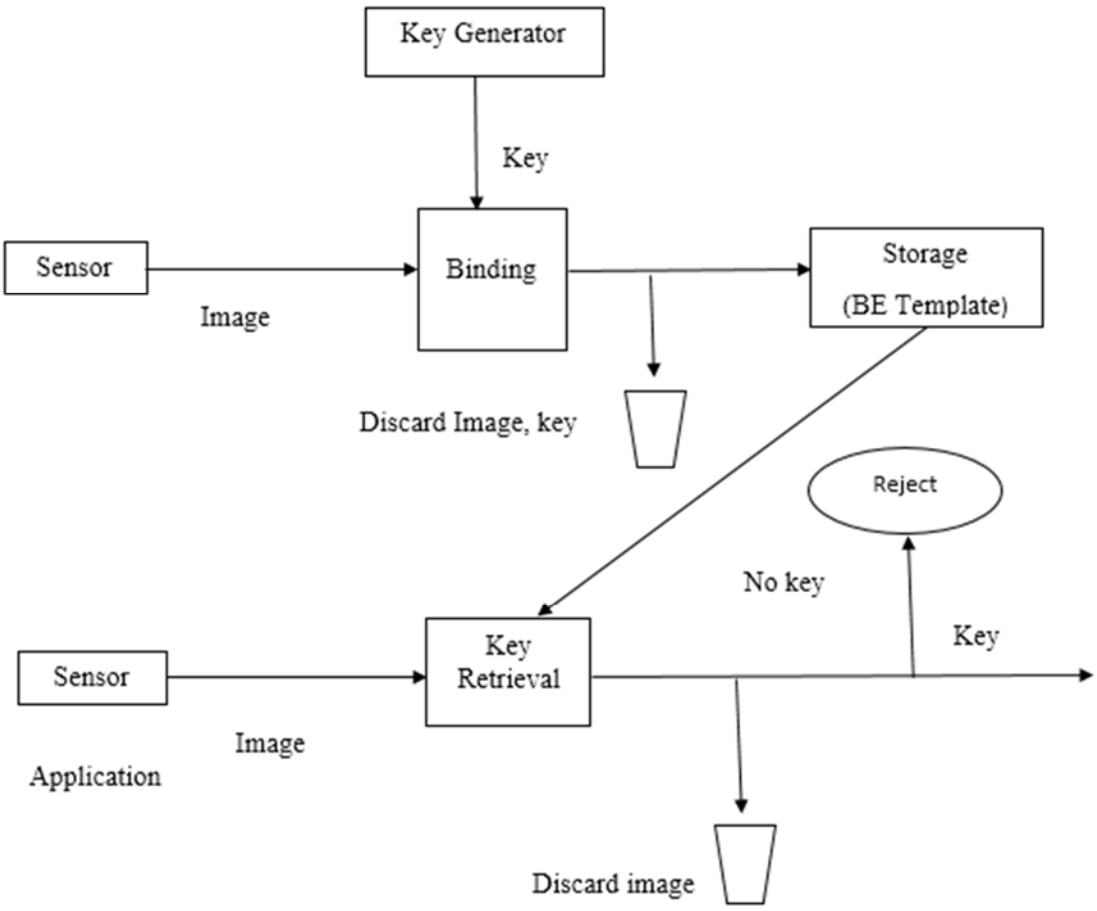


Figure 1. High level diagram of a biometric encryption process.

As shown in *Figure 1* , in the key binding mode, a random key will be generated during the image capturing. This key is completely independent of the user's biometric sample.

The biometric encryption algorithm securely binds the key from the biometric sample to create a biometrically encrypted key. Basically, the biometric encryption template provides privacy protection and can be stored in either a database or other electronic accessories. At the end of the process, the biometric sample and generated key are discarded [20].

During the verification time, when the user presents his or her biometric sample to the system, the key values are compared with the previously stored key or template image. Then the key or image will be retrieved from the storage to allow the person to access. At the end of the verification, the retrieved key or image will be discarded again [19]. This algorithm is designed to accept a slight variation of the given input samples. On the contrary, if the sample keys are not matched with each other, the system will automatically reject the input.

Advantages of Biometric Encryption Process

Fingerprint biometric has huge potential to enhance privacy and security [14]. Some key advantages of this approach include:

No retention of biometric template image. Many privacy and security concerns derive from storage and misuse of the biometric data.

Cancellable, various, resilient identifiers. Biometric Encryption allows people to use one biometric for numerous accounts. If an account identifier becomes compromised, there is not much risk that all the other accounts will be as well, i.e., no need to change one's fingers.

Enhanced validation security. No need for user memorization and less vulnerable to security attacks.

Enhanced security of individual data and communications. Since the key is one's own biometric, this technology could place a reliable tool in the hands of users.

Biometric Encryption to the Prototype Stage

Biometric Encryption has been researched since the mid-90s. Scientifically, this area is much more stimulating than conventional biometrics [15]. As shown in the *Figure 1*, there are several steps involved in the prototype stage.

Select a proper biometric. Fingerprints Biometric Encryption was first pioneered, making it a prime choice. Since then, it has been used more extensively than the other biometrics such as facial or iris recognition. In addition, maximum privacy concerns navigate the use of fingerprints.

Increase the image acquisition process. Selecting a proper fingerprint sensor reduces the amount of skin distortions [12]. Image quality can also be enriched at the algorithm level.

Make biometric encryption resilient beside attacks. By chance, if an attacker has access to both the Biometric Encryption templates and the algorithm, they should not able to access the biometric, even if they are fully aware of the algorithm.

Expand the accuracy and security of the biometric encryption algorithm. Progress is being made that is relevant to Biometric Encryption.

Achievement of a multimodal approaches. When different types of algorithms, fingers, or biometrics are combined, the performance of a biometric system is expressly enriched. Therefore, the modes that were shared must be orthogonal (Statistically Independent).

Improved biometric encryption applications. To exhibit the benefits for privacy and security, we are using Biometric Encryption.

Use of biometric encryption in the united states government. Some of the biometric applications are given below:

- FBI-Integrated Automated Fingerprint Identification System (IAFIS)
- US-VISIT Program
- Transportation Security Administration (TSA) Registered Traveler Program
- U.S. National Science and Technology Council's Subcommittee on Biometrics

Privacy and Security Issues Involving a Biometric System

By using biometrics, anyone can keep their data as secret and private. As shown in *Figure 2*, this system explains how the template image has been stored and the data is kept in secret [20].

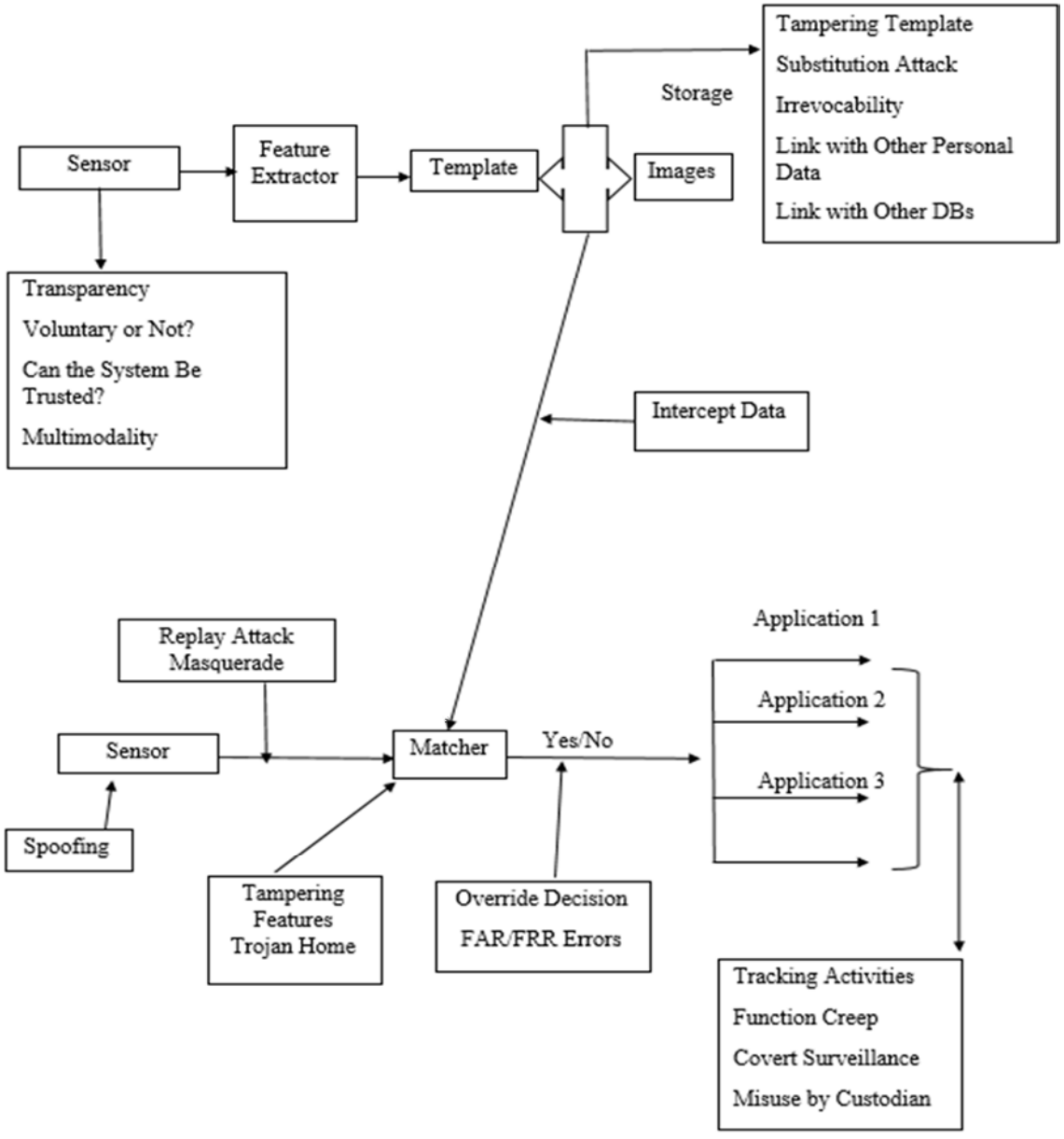


Figure 2. Privacy and security issues involving a biometric system.

The major issues involved in the biometric system are shown in *Figure 2*.

Spoofing: A biometric system sometimes can be fooled by applying fake fingerprints.

Replay attacks: A previously recorded image will be applied into the system, instead of giving an original one.

Masquerade attack: An artifact image can be drawn from the fingerprint template. Thus, whenever a person applies their fingerprint, the system will produce a match.

Tampering: An attacker will modify the templates to obtain a high verification score during the matching process. So, the system will be matched with all the given input data.

Trojan horse attacks: If the matcher is attacked by Trojan horse, all given inputs will result in a high verification score.

Substitution attack: Typically, the template is stored in the database so the system must allow user verification. As an example, suppose an attacker were to get access to the template storage, he/she can modify the user's template to match with their own finger.

Overriding Yes/No response: The output of the system is always a binary Yes/No (i.e., match/no match) response.

Insufficient accuracy of many commercial biometric systems: High False Recognition Rates causes inconvenience for users to lower a verification threshold. This gives rise to False Acceptance Rate, which, in turn, lowers the security level of the system.

Biometric Identification vs. Verification

To find an individual's biometric record from the large set of biometric records is called identification [1]. For instance, the fraud detection system checks the person's identity such as face, iris etc., and compare with the database to ensure that multiple documents had not been handed out to the same application to receive a person's passport or driver's license.

The process, wherein a biometric sample is compared with the samples stored in a database is called verification or authentication. For example, a person can see their identity card's serial number, however, the number must be matched with the database where the data has been previously stored. In this way, the system knows the bearer holding that card, and is allowed the access or not.

In some cases, such as passport applications, both identification and verification are required. Firstly, a *one-to-many* search (for e.g., a person's background verification) is performed to make sure that a person has not been listed in certain databases such as criminal/terrorist list. Once the person clears all the preliminary requirements, the person's identity is stored in a *one-to-one* system [10].

Authentication Process Based on Cancellable Biometrics

Although, the biometrics are more secured than the other system, the stored template images from the database can be stolen as shown in *Figure 3.* The concept of cancelable biometrics helps to create a biometric template that can be cancelled. A distorted version of the biometric template is stored, which provides high privacy level by allowing multiple templates to be associated with the same biometric data.

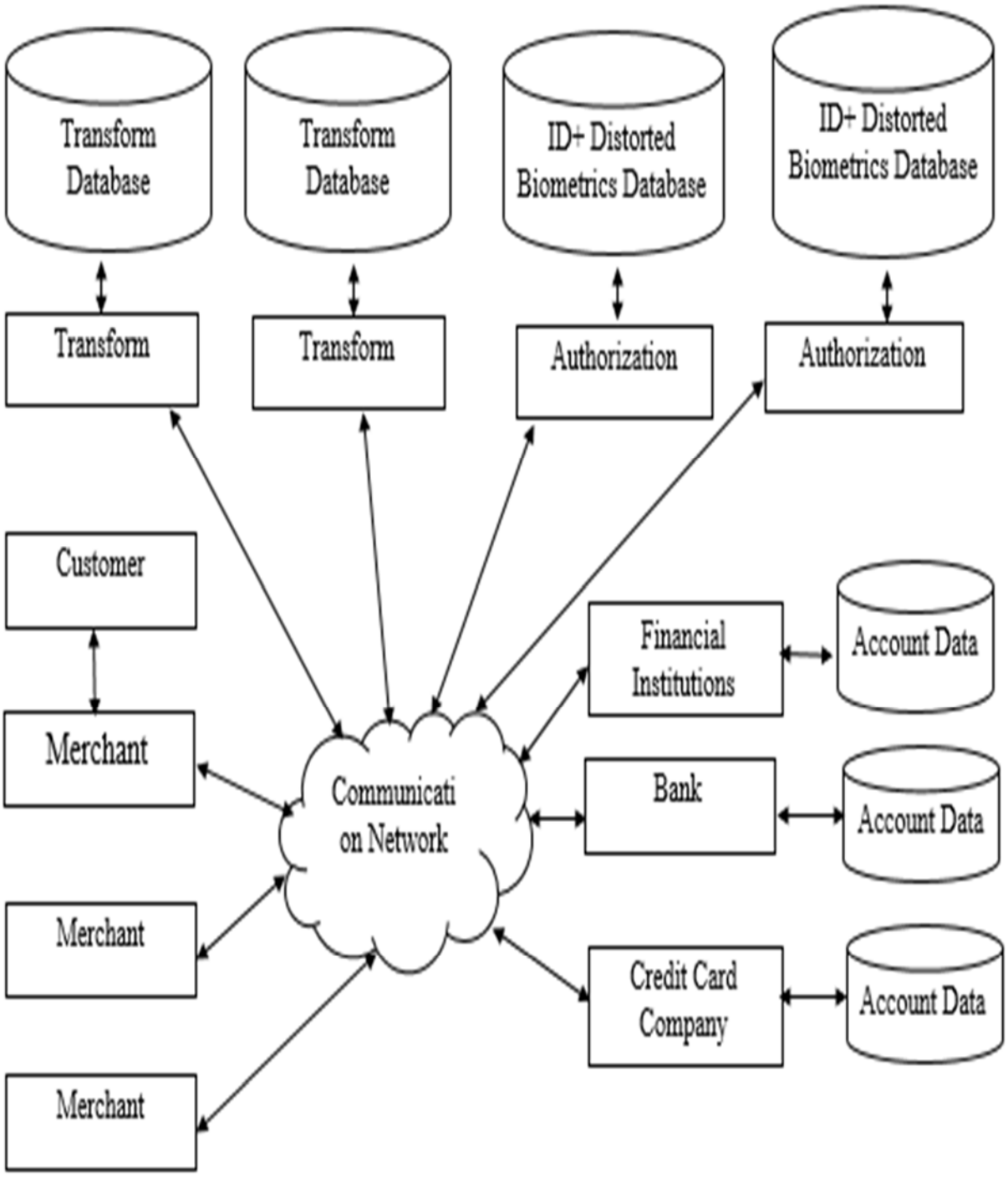


Figure 3. Authentication Process Based on Cancellable Biometrics (source: Encyclopedia of Biometrics).

These are the following applications; we are using it for the authentication process based cancellable biometrics.

Government: Passports, national identification (ID) cards, voter cards, driver's licenses and social services.

Transportation: Airport security, boarding passes, and commercial driver's licenses.

Healthcare: Medical insurance cards, patient/employee identity cards.

Financial: Bankcards, ATM cards, credit cards, and debit cards.

Security: Access control and identity verifications, including time and attendance.

Education: Student/teacher identity verification and access control.

CHAPTER 2: FINGERPRINT BASED IDENTIFICATION

Multimodal Biometrics

There are about 18 different models of biometrics in the recognition method as shown in *Figure 4*. However, the most commonly used techniques are fingerprint, iris and face [12].

Figure 4. Multimodal Biometrics.

Fingerprint recognition are the most common available technology in the biometrics. Fingerprints exits throughout biometric applications, because of its uniqueness, resolution and ease of achievement.

As shown in *Figure 5*, there are different categories of fingerprint structures on the fingertip lines such as arch, tented arch, right loop, left loop and whorl. There are about 65% of Loop, 30% of Whorl 5% of Arch in a human's finger [17].

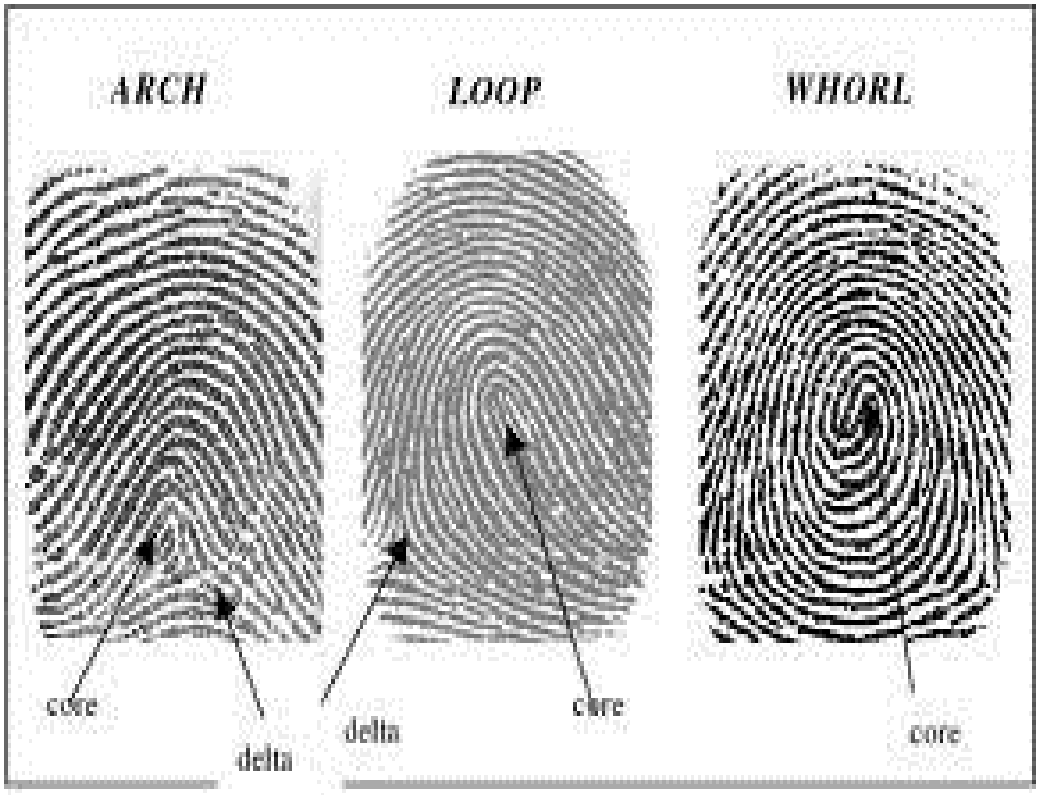


Figure 5. Arch, Loop, Whorl.

Existing User Authentication Techniques

Although fingerprints are authenticated, there are several ways to confirm the person is who they say they are as shown in *Table 1*. The following terms are what the system is looking for:

- What You Have
- What You Know
- Who You Are

A system that has stored information, such as identity card and passport is called "*what you have.*" Having pin number and password to access like an ATM is called "*what you know.*" The system which is looking for physical evidence that you are who you say you are is called "*who you are,*" for instance, fingerprint, iris and vein geometry.

Table 1.

Existing User Authentication Techniques. (Source: eds.com)

Method	Examples	Properties
What you Know	User ID Password PIN	Shared Many Passwords Easy to Guess Forgotten
What you Have	Cards Badges Keys	Shared Can be Duplicated Lost or Stolen
What You Know and What You Have	ATM card + PIN	Shared PIN a week link (Writing the PIN on the Card)
Something Unique About the User	Fingerprint Face Iris Voiceprint	Not Possible to Share Repudiation Unlikely Forging Difficult Cannot be Lost or Stolen

Fingerprint Based Identification

As shown in *Figure 6*, an image of the fingerprint is captured by a scanner or sensor, then it will enhance the image quality, and convert it into a template. Scanner technologies can be optical, silicon, or ultrasound technologies. Typically, optical scanners are the most commonly used. During enhancement, noise caused by cuts, scars, dryness and wetness in fingerprints is reduced, and the ridges are enhanced.

Figure 6. Image processing method.

These are some of the benefits of fingerprints:

- It is very difficult to fake fingerprints, unlike identification cards
- A fingerprint cannot be stolen (but the digital equivalent can)
- Signatures can be easily copied; fingerprints are more difficult to copy

Ridges and Valleys on a Fingerprint Image

A Fingerprint layer is a skin particle on your fingertip. The structure of fingerprint has separated in two ways: ridges and valleys. Typically, ridges and valleys looks like a parallel but, they split or dismiss most of the time.

There are about 150 different types of minutiae that are characterized based on their shape [10], but the most commonly used methods are Ridge ending and Ridge bifurcation points as shown in *Figure 7*.

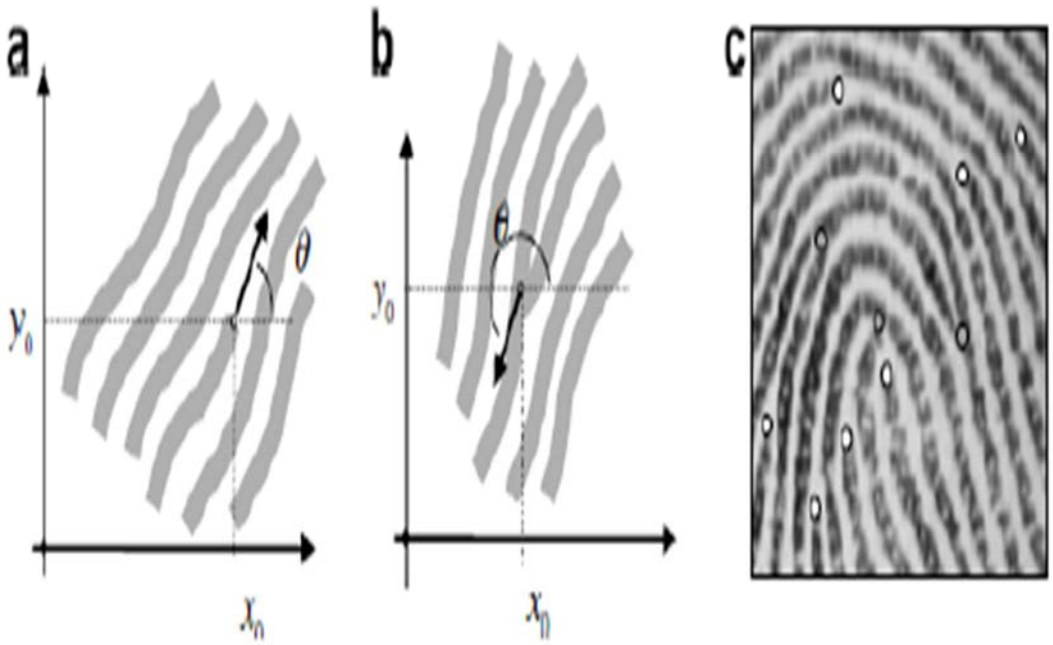


Figure 7. (a) A Ridge ending (b) Ridge bifurcation (c) Termination (white) and Bifurcation (gray) Minutiae in a sample fingerprint.

A small scratch, scrape, or even burn will not affect the structure of ridges of the fingerprint. The newly developed skin will form in the original place within a short period. Although, it causes some minor problems in that area, it will not affect the fingerprint itself. Ridges are connected to the inner skin by small projection called papillae. If, suppose, the papillae are smashed, the ridges are done for and the fingerprints are wrecked.

Fingerprint Recognition Using Standardized Fingerprint Model

A shown in *Figure 8*, first the fingerprint image is preprocessed and it converts the image into binary. Then the *morphological operation* will be applied to get a thinning image. Finally, the minutia points are extracted and their corresponding values are found.

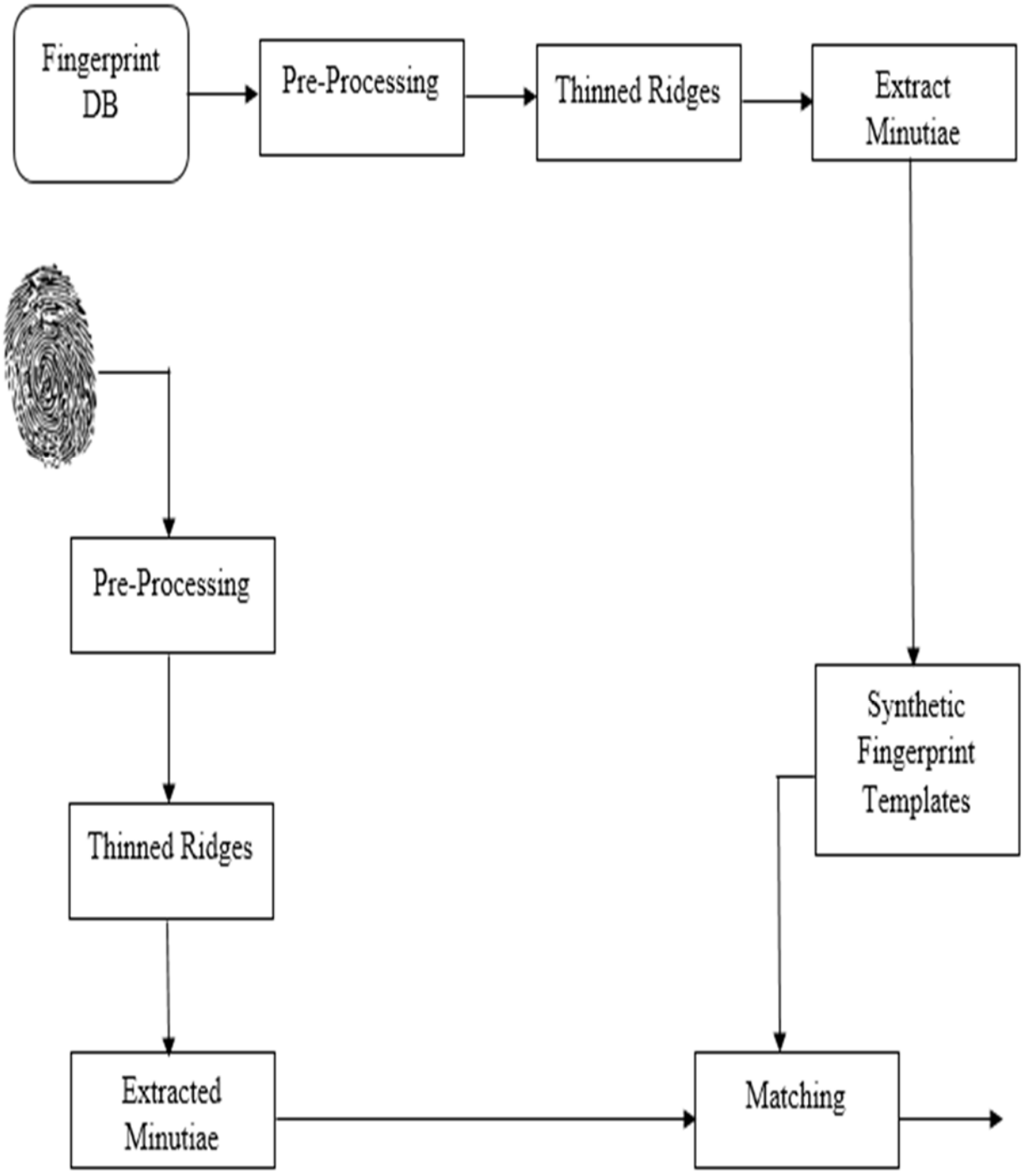


Figure 8. Fingerprint Recognition using standardized fingerprint model. (source: Thai & Tam)

Fingerprint Recognition Steps

As shown in *Figure 9*, there are three steps involved in this model: (i) pre-processing, (ii) minutiae extraction and (iii) post processing.

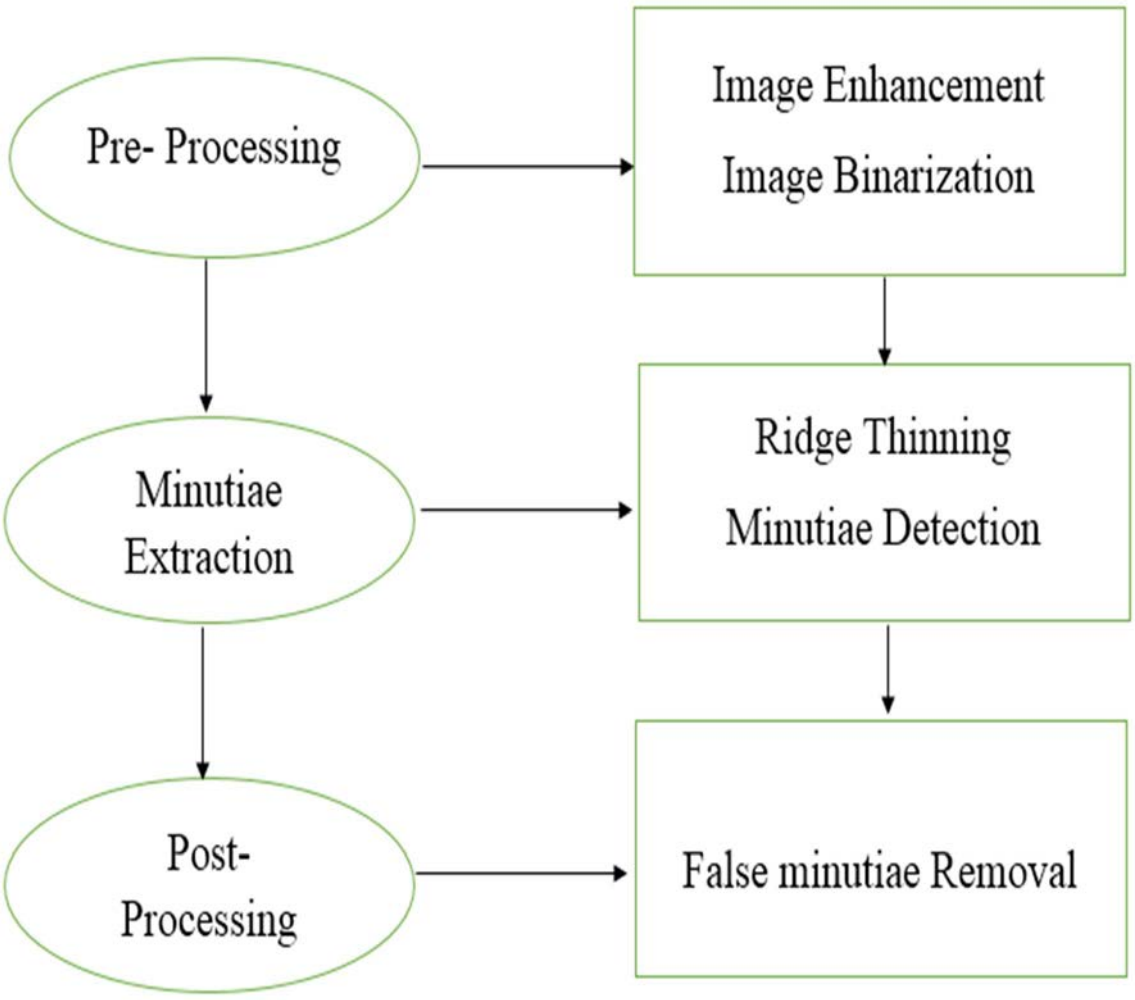


Figure 9. Fingerprint Recognition Steps.

Pre-processing

During the pre-processing stage, the captured image will be enhanced by a histogram function. Later, if there is any noise in the image, the noise will be removed by using image filtering techniques such as Gaussian, Speckle, Salt & Pepper noise. Furthermore, the image will be sharpened to find the edge detection of the enhanced image.

Edge occurs in the boundary between two different regions in an image. To find edges in a given image we use Prewitt, Sobel and Canny. Canny is the most commonly used method for edge detection [12].

Image Enhancement

Adjusting a digital image makes it more appropriate for exhibition or supplementary image analysis as shown in *Figure 10*. During the image enhancement process, the image will be sharpened, brightened, and noise will be removed to identify the key features.

Histogram equalization model for fingerprint image. As shown in *Figure 10,* by using a histogram technique for a particular image, a person can observe the whole distribution at a glance. The images are displayed in both bright and dark of their corresponding pixel values for both background and foreground areas. [10]

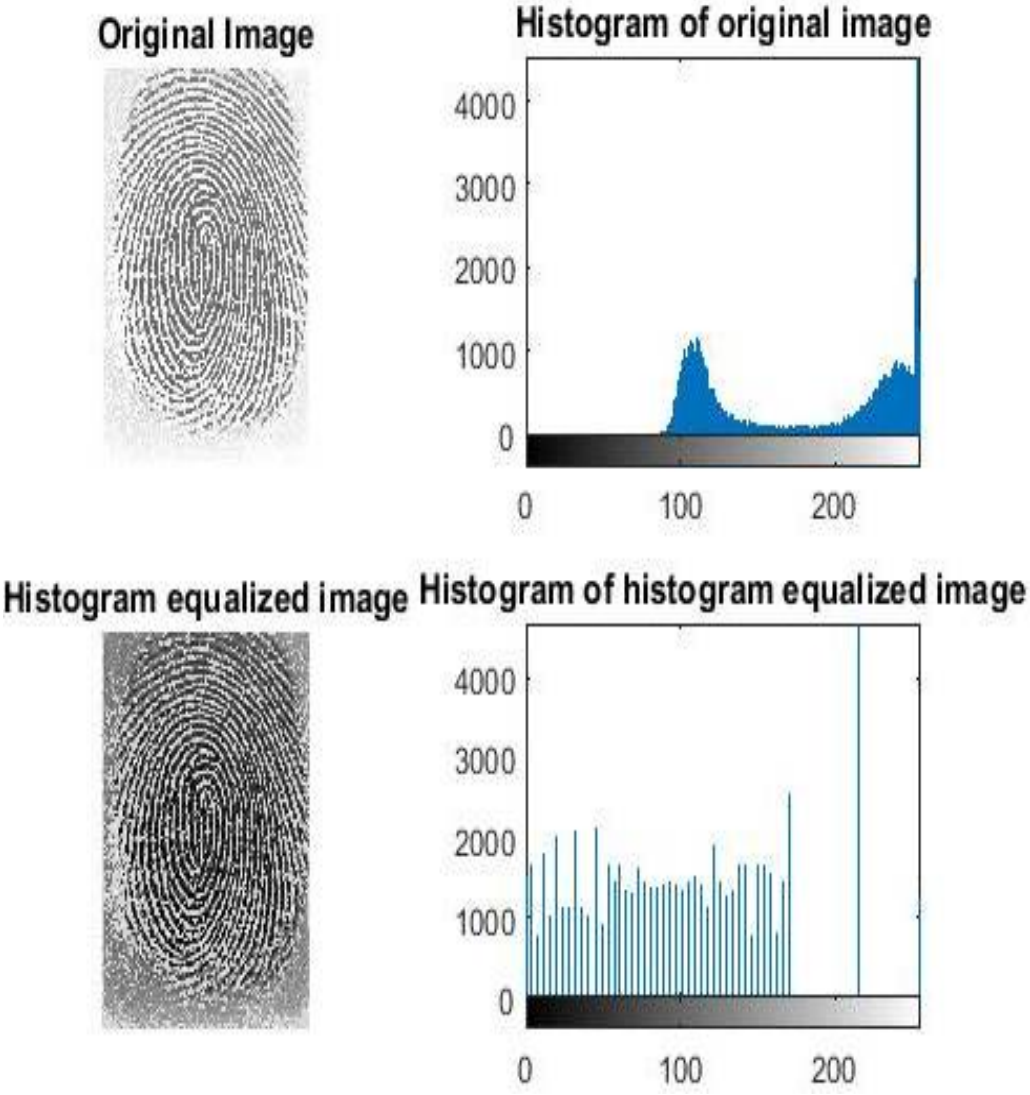


Figure 10. Histogram Equalization model for fingerprint image.

Image Filtering

Filtering is a technique for adjusting or enhancing an image to highlight certain features or eliminate other features. There are three ways to perform the filtering as given below.

- Low Pass Filters (Smoothing, Blurring)
- Moving Window Operations
- High Pass Filters (Edge Detection, Sharpening)

Low pass Filter

A Low pass filter is a technique which only calculates the average of a given image pixel and all its eight neighbors. So, the original values are replaced by the resulted pixel. The same steps will be applicable for each pixel in the given image.

Smoothing. It is very helpful to remove the noise form the image without changing their original edge values.

The blurring. The during the image blurring or degradation is placed when the image is captured from the camera. It could be either out of focus or a movement capture time.

Moving Window Operations

By changing the pixel values in the region, this operator will move over the image to affect all the pixels in an image. Initially, the operator only focuses on one pixel at a time.

High Pass Filter

It is a reverse method of a low pass filter. To emphasize certain pixel details in the image, a high pass filter is used in this research. It will also make an image very sharp in order to detect the true edges.

Noise Removal

Image noise is a function which will be placed during the image capturing time in the sensor. Basically, noise is caused by cuts, scars, dryness, or wetness in fingerprints. The noise will produce a random variation in images like brightness and color information as shown in *Figure 11*. To remove the noise, we are using Gaussian, speckle and salt & pepper noise.

Figure 11. (a) Gaussian noise (b) Speckle noise (c) Salt & pepper noise.

1. Gaussian kernel noise is very useful to find edges in the image and smooth the surfaces.

2. To multiply pixels with a random value of integers is called speckle noise, which is also known as multiplicative noise.

3. The most commonly used technique to remove the noise is salt & pepper. It is also known as impulse noise. The impulsive noise will be caused by sharpening, and unexpected distributions in the image signal. If the neighborhood value is “0” and isolated value is “1”, it is salt. In reverse, if the neighborhood value is “1” and isolated value is “0”, it is pepper noise.

Sharpening & Edge Detection

Edge detection. Edges are significant local changes of intensity in the image. This typically occurs in the boundary between two different regions in an image. As shown in *Figure* 12, important features can be extracted from the edges of image (e.g., curves, lines, corners). Basically, these features will be used in computer vison algorithms. There are different methods involved in finding the edges in the image surface such as Prewitt, Sobel and Canny.

Prewitt. Edges are measured by using transformation between corresponding pixel intensities of an image.

Sobel. To find the approximate absolute gradient magnitude at each given input grayscale image values.

Canny. Here the input value is a gray scale image, then it will produce the output image as places of tracks in intensity discontinuities.

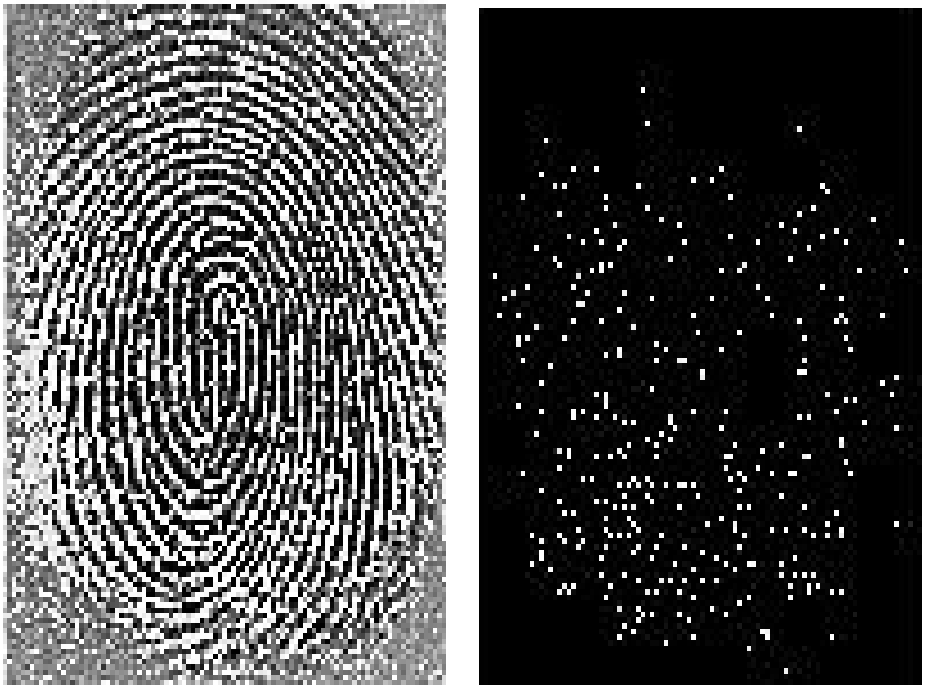
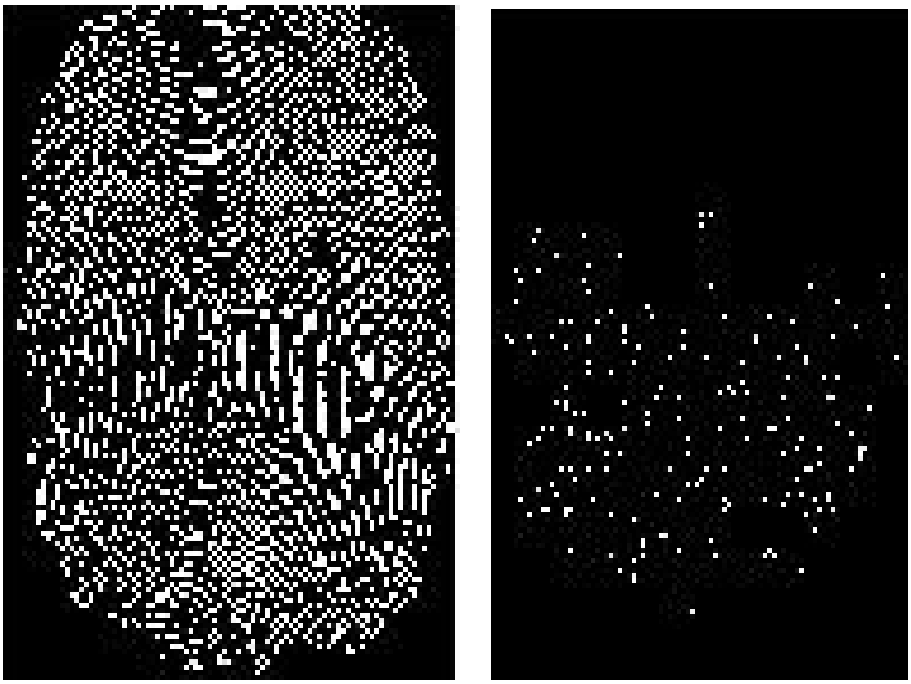


Figure 12. (a) Sharpen image (b) sobel



(c) canny (d) prewitt edge detector.

Image Binarization

There are two different ways to threshold the binary image. These are:

- Binarize Image Using Global Threshold
- Binarize Image Using Locally Adaptive Thresholding

Figure 13. Adaptive threshold value for the binary image.

To segment objects from a background is known as thresholding. If the background pixel values are relatively uniform, then global threshold is used to binarize the image by using its corresponding pixel intensity. Alternatively, if the background intensity values have a large variation, then the adaptive threshold is used as in *Figure 13.*

Minutiae Extraction

Ridge thinning and Minutiae detection. A thinning process is used to remove particular portions of foreground pixels in the binary image as shown in *Figure 14*. Thinning is a morphological operation and it is widely used in many applications. In particular, it is very useful for skeletonizing. Here we are using it for cleaning up the resultant output of edge detectors.

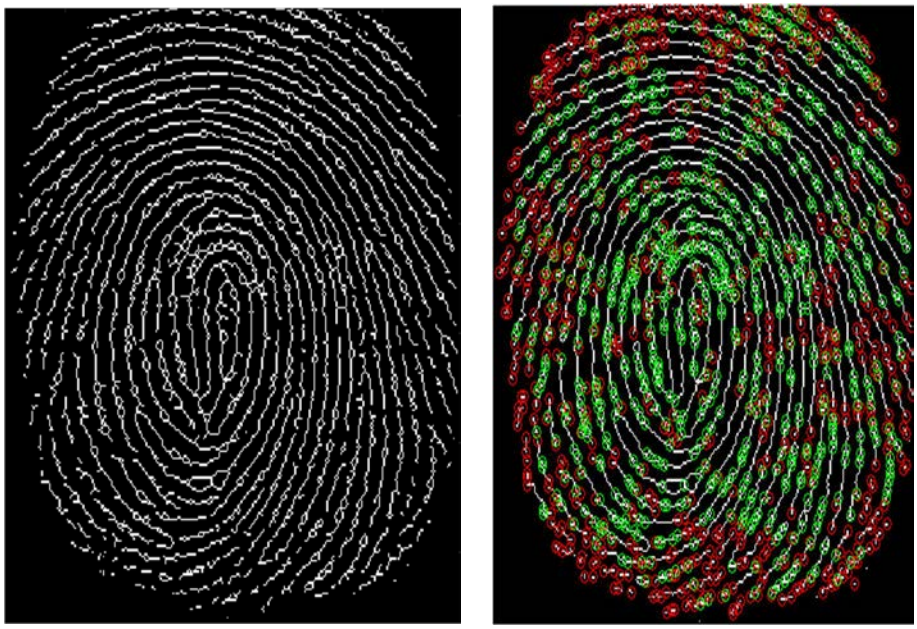


Figure 14. (a) Ridge thinning (b) Minutiae detection (source: Florence).

Human fingerprints have many details when the skin layer is pressed in a smooth surface [10]. It is commonly denoted as minutiae. Ridge ending and ridge bifurcations points are most commonly used minutiae techniques for identifying a human finger.

There are three techniques involved in this method as given below.

Minutiae extraction technique. Minutiae extraction technique is the most commonly used technique in the biometric process. If the two given minutiae points are matched with each other, then it is classified as same finger.

Pattern matching or ridge based technique. Compared with the above technique, pattern matching is very sensitive to proper settlement of the finger and it needs a large space for template storage.

Correlation method. Two fingerprint images are placed over and the correlation between corresponding pixels is computed for various displacements and rotations.

Crossing Number. Crossing number is a commonly used technique in minutiae extraction. A skeleton image contains eight neighborhoods of its ridge patterns. T he neighborhood of each ridge pixel in the minutiae model is scanned by using a 3×3 window operation. Now the crossing numbers are computed by half the sum of the 8 neighbor's pairs, as shown in *Table* 2 and *Table 3*. The ridge pixels are classified as ridge ending, and bifurcation points with their corresponding values. For instance, the crossing number value "1" represents the ridge ending point and the crossing number value "3" represents the bifurcation point.

Table 2. Crossing number properties.

Property	**Crossing Number**
Isolated Point	0
Ridge Ending Point	1
Continuing Ridge Point	2
Bifurcation Point	3
Crossing Point	4

$$CN = 0.5 \sum_{i=1}^{9} |P_i - (P_{i+1})|, \; P_9 = P_1 \qquad \text{(Equation 1)}$$

where P_i is the pixel value (where possible values are 0 and 1) in the neighborhood of P. For a pixel, P, its eight neighboring pixels are represented in an anticlockwise direction as follows in the *Table 3.*

Table 3. (a) Eight neighboring pixels (b) ridge ending (c) bifurcation point.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

0	0	1
0	1	0
0	0	0

0	1	0
0	1	0
1	0	1

Post-Processing

False Minutiae removal. No two fingerprints are exaclty alike, but their ridges might be equal with furrows. To solve this, we are using a 3×3 matrix which previously stores each ridge and furrow in a separate dataset. This result will help to find if the two different fingerprints are distinctively unique with their corresponding key vector elements as shown in *Figure 15 and Figure 16* .

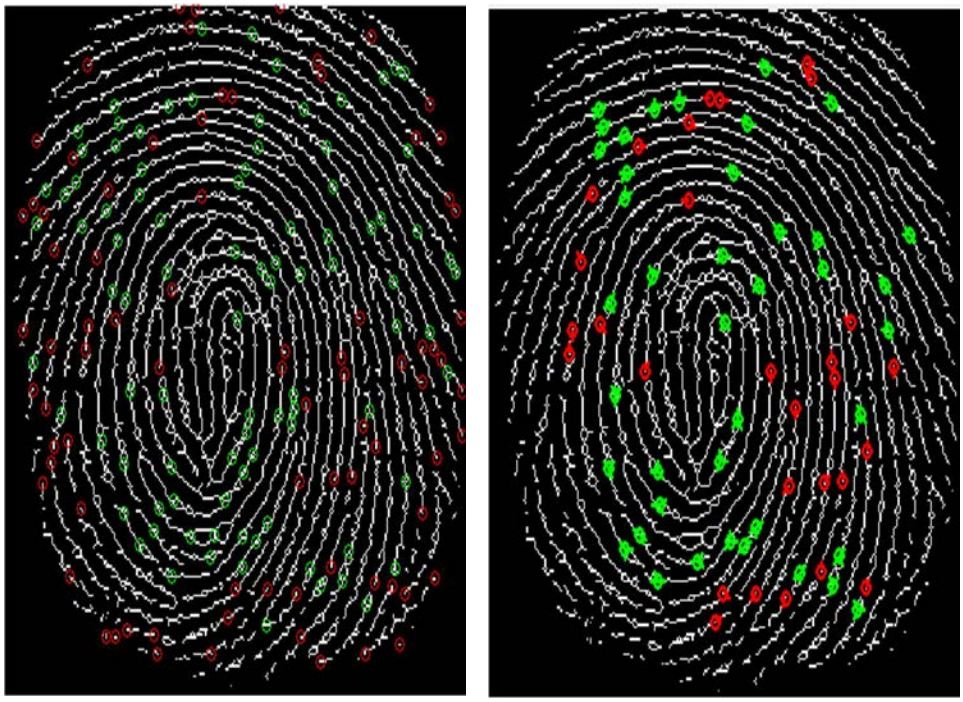


Figure 15. (a) Minutiae Detection Points (b)False Minutiae Removal.

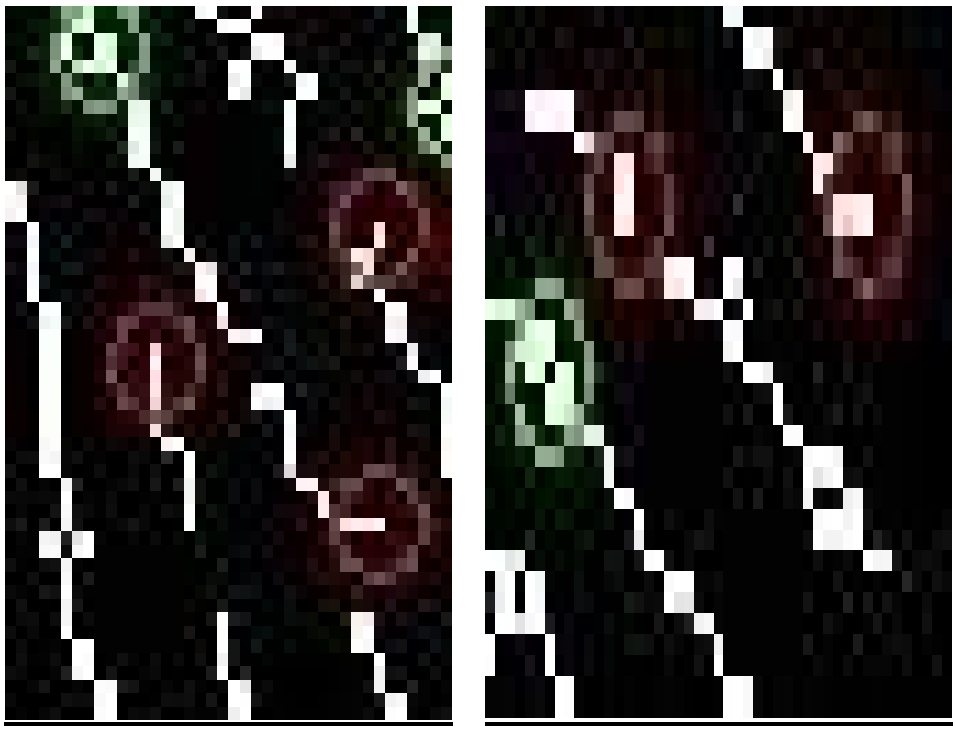


Figure 16. (a)False minutiae point 1 (b) False minutiae point 2

CHAPTER 3: CRYPTOGRAPHIC KEY GENERATION FROM BIOMETRIC

Cryptography is the science of secret writing which is very helpful in communicating over the networks such as the internet. There are five primary functions of cryptography today [21] as given below:

Privacy / confidentiality. Ensuring that no one read the message except the intended receiver.

Authentication. The process of proving one's identity.

Integrity. Assuring the receiver that the received message has not been altered in any way from the original.

Non-repudiation. A mechanism to prove that the sender really sent this message.

Key exchange. The method by which crypto keys are shared between sender and receiver.

Basically, a cryptosystem has many problems associates within such as:

1. Typically, messages are based on the key in cryptography. So, the system may fail to differentiate whether it is used by a hacker or the legitimate user.
2. The keys are easily broken or predicted in Cryptography.
3. Encryption and decryption process will take longer time if the key values are larger than usual.

4. To remember the key is very tedious. At the same time, storing that key in database is another uncertainty.
5. Furthermore, sharing a lengthy or random key will generate a problem in the cryptography system.

To solve the above-mentioned problems, we are using a biometric cryptosystem. Basically, combining cryptography and biometrics together is known as *biometric cryptography*.

By using this method, cryptography will provide the high security level and biometrics will help to avoid remembering passwords. In addition, the cryptographic keys are generated from the user's biometric templates. Unless the same person participates again, the system will not reveal the previously stored keys for verification [3].

There are several types of cryptosystems available for biometry applications such as key release, key binding and key generation cryptosystems [6].

In the key release cryptosystems, the key will be released after the given biometric sample is verified. Initially, the cryptographic key and the biometric data are separated from each other. It might get affected by some harmful software during the authentication time. Because the authentication and the key release are independent, this process will not be suitable for many applications.

In the key binding cryptosystems, the biometric data and the cryptographic keys are combined. So, the key will not be generated unless the same person is involved in the system.

In the key generation cryptosystems, the secret key will be generated by a special algorithm for given biometrically extracted points. Comparatively, this system is distinguished from the other models because the database will not store the cryptographic key in this system.

Application of Biometric Encryption Cryptosystem

Several pieces data and information are needed to be protected and secured from the user. In order to achieve this, the biometric encryption method is used in many applications as listed below:

Border security control. These days, many people are travelling around the world. So, the identification requirement plays an important role in the airport and border crossing to collect the traveler's fingerprint, iris patterns and facial images.

Crime and fraud prevention, detection, and forensics. Using biometrics such as a fingerprint, can be digitized, recovered and verified rapidly. In this way, it is convenient to monitor and check a person's backgrounds. Also, it will help to solve crimes, and make the world a better place to live.

Attendance recording. Due to the increased number of people in an organization, the sign-in or registration methods are necessary. In this case, biometrics are helpful to solve this problem. By using this, a person's fingerprint or hand can be taken by the system and it will register and allow the person to access the building, premises etc.

Payment systems. Using biometrics in everyday life is more feasible than any other method. For example, when shopping in for groceries or gasoline, a person can use their fingerprints instead of card or cash.

Access control. Biometrics are more secure than any other system. For instance, applications are wrecked or lost when someone uses it for a long time. But biometrics are not even broken or damaged. For example, accessing laptop gets more secure by using biometric method.

Cryptographic Key Generation Algorithm

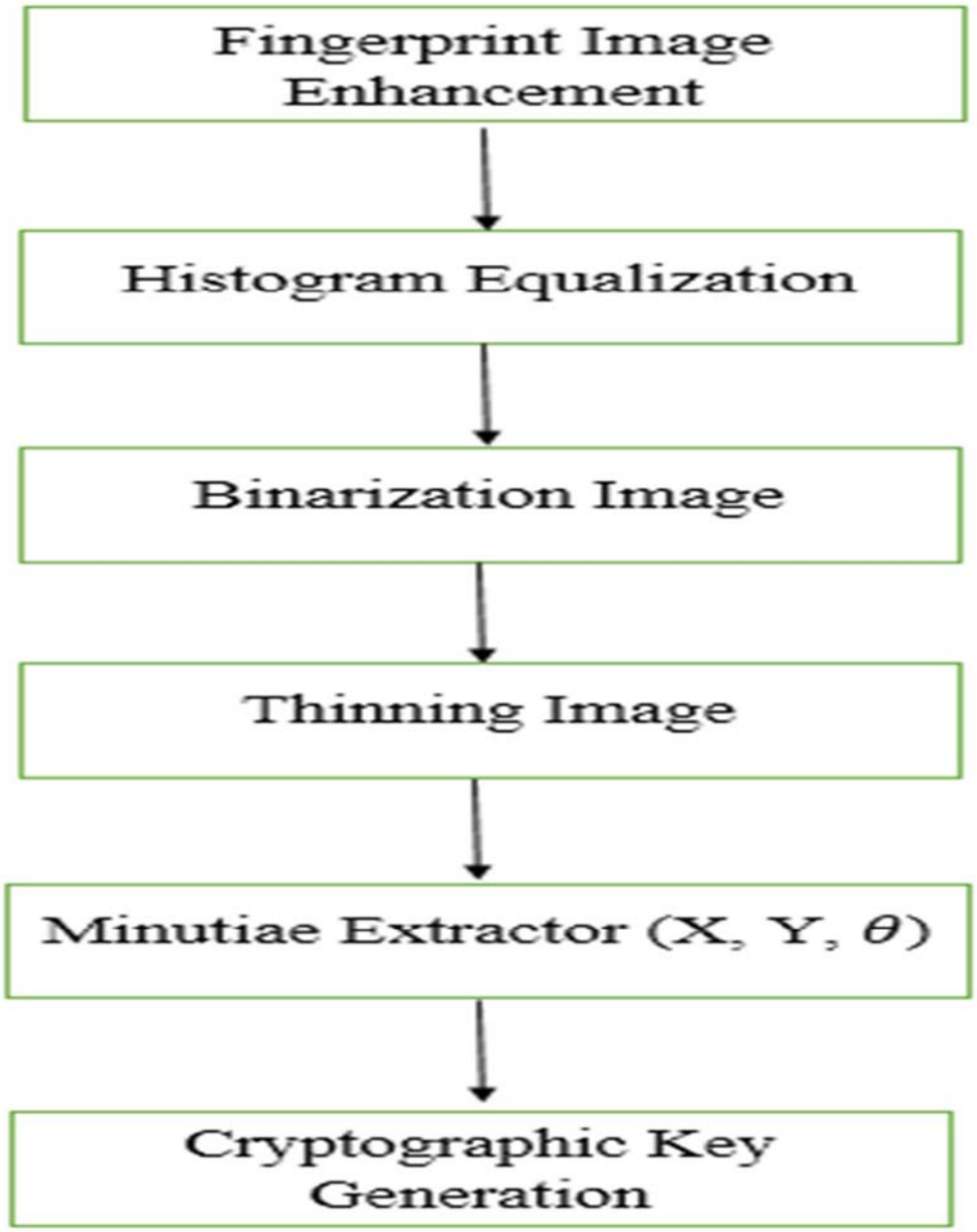


Figure 17. Block diagram of cryptographic key generation. [17]

The cryptographic key generation algorithm is as follows.

As we discussed in*Table* 2, the minutiae coordinate and angles are measured and data values are extracted as shown in *Table 4*. In addition, Ridge Ending (RIG) is marked in red, and Bifurcation (BIF) is marked in green as shown in *Figure 18.*

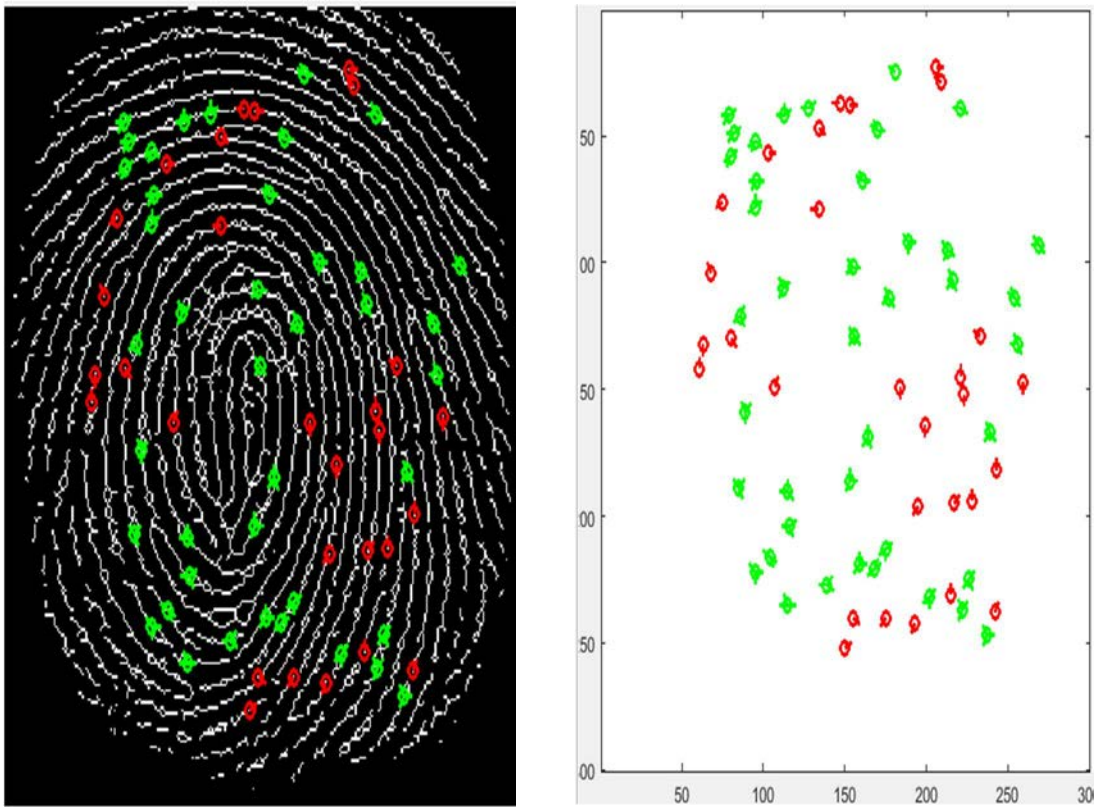


Figure 18. True Minutiae Sets.

The average values of minutiae point X and Y coordinates and angle θ are calculated. The resultant outputs are in decimal for X and Y coordinates and radians for angle θ as shown in *Table 4* . These output values are converted into binary representation, because during the

preprocessing time the input image values are resized into 256x256 array for minutiae extraction [17].

Lastly, all the binary values are converted into single coordinate values. By concatenation of these three values, a private key will be generated for the given fingerprint image [17]. The algorithm steps are given below:

I. : Get the binary values $XBi, YBi\ and\ \theta Bi,$

$Xi, Yi\ and\ \theta i\ for\ i^{th}$ given minutiae.

II. : Concatenate all the binary values in the following order.

MBi = X and Y Locations are (28 bits each) + angle θ (8 bits).

III. Convert the above concatenated binary string MBi to decimal to get the single co-ordinate value $M1i$.

Table 4. Minutiae co-ordinates and angle values. (source: NIST)

X	Y	θ	Minutiae Type
61	291	0	3
64	132	4	1
65	271	16	3
83	214	18	3
85	160	4	3
96	161	20	3
105	115	21	3
116	145	20	3
133	279	14	3
135	288	13	1
140	282	29	3
154	181	2	3
163	339	11	3
163	380	25	3
175	70	23	3
177	353	25	3
184	82	24	3
186	330	9	3
188	123	23	3
192	25	24	3
192	262	31	3
193	13	24	3
193	57	24	3
195	151	7	3
196	167	22	3
197	72	8	3
198	219	1	3
199	118	8	3
202	55	8	3
203	87	24	1
203	240	16	3
205	80	8	3
207	25	8	3

207	336	23	3
208	311	6	3
213	317	22	3
214	147	24	3
214	258	1	3
216	14	9	3
219	208	17	3
223	166	8	1
225	65	9	3
237	371	4	3
239	177	28	1
242	150	27	3
258	337	19	3
269	94	26	1
280	176	14	3
285	273	18	3
294	111	27	1
300	28	10	3
306	59	27	1
306	215	31	3
307	228	16	3
311	354	3	3
316	148	13	1
318	93	11	1
319	353	19	3
349	228	31	1
351	272	16	3
355	174	14	3
361	266	16	3
371	72	12	1
374	305	0	3
385	98	12	3

The algorithm results for the original fingerprint image values are given below.

X = 14320/65 = 11010010000110100000011101100

Y = 12171/65 = 10110010100100100011001001001

Theta θ = 1027/65 = 10011110

The generated cryptographic key of length 64 for the biometric image in *Figure 18* is as follows:

1101001000011010000011101100101100101001001001100100100110011110

The original image, the encrypted image and the output image respectively are shown in *Figure 19* .

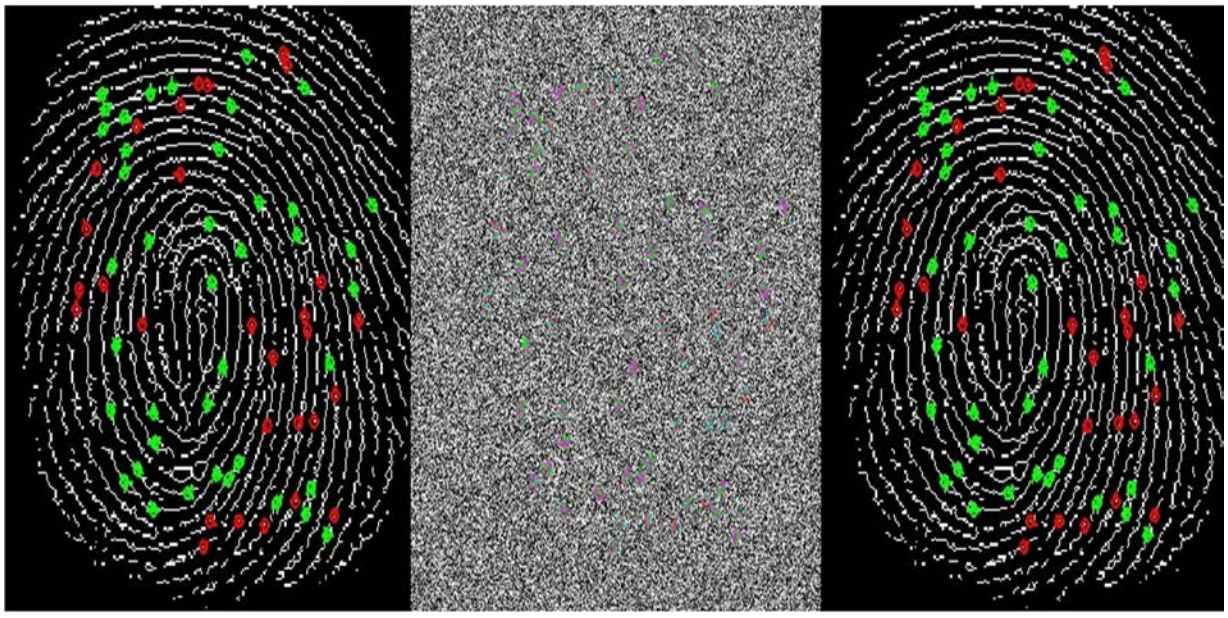


Figure 19. Cryptographic based Encrypted and Decrypted image.

SUMMARY

This research proposes the use of fingerprint samples to generate a cryptographic key for increased security. There are many biometric samples available for use in this recognition model; however, the fingerprint was selected as the biometric. Fingerprints are stable and remain consistent throughout a person's lifetime. Initially, the captured image is converted to a binary representation. Then, minutiae points are extracted by using a MATLAB function. Next, the cryptographic keys are generated from the corresponding minutiae values. During this work, it was discovered that each person has unique minutiae coordinates, and orientation angles. The proposed method can be used as an efficient biometric security system for application such as online banking, border security control, forensics etc.

FUTURE WORK

The matching process between the fingerprint and other templates by using database FVC2004 DB4, which contains a very low image quality to demonstrate the ability of the proposed model.

Modify the existing algorithm for fingerprint identification such that the image quality can be improved to achieve high security.

Exploring the possibility of implementing the fingerprint identification process on Field Programmable Gate Array (FPGA) for higher performance.

Furthermore, by utilizing the parallel processing capabilities of FPGA, the overall computational speed of the algorithm can be improved.

REFERENCES

[1] C. Saraswat and A. Kumar, "An Efficient Automatic Attendence System Using Fingerprint Verification Technnique," in *Chitresh Saraswat et al*, 2010.

[2] S. Greenberg, M. Aladjem, D. Kogan and I. Dimitrov, "Fingerprint Image Enhancement Using Filtering Techniques".

[3] A.Jagadeesan and Dr.K.Duraiswamy, "Secured Cryptographic Key Generation from Multimodel Biometrics: Feature Level Fusion of Fingerprint and Iris," in *International Journal of Computer Science and Information Security*, 2010.

[4] A.Jaya Lakshmi and I. Ramesh Babu, "Design of Secured Key Generation Algorithm Using Fingerprint Based Biometric Modality," in *IOSR Journal of Engineering*, 2012.

[5] Colin Soutar, Danny Roberge, Alex Stoianov, Rane Gilroy and B.V.K. Vijayakumar, "Biometric Encryption," in *Bioscrypt Inc*, Mississauga, ONT.

[6] Dr.R.Seshadri and T.Raghu Trivedi, "Efiicient Cryptographic Key Generation Using Biometrics," in *Int.J.Comp.Tech.AppL*.

[7] G. T. Candela, P. J. Grother, C. I. Watson, R. A. Wilkinson and C. L. Wilson, "PCASYS - A Pattern-level Classification Automation System for Fingerprints," 1 August 1995. [Online]. Available: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=900754. [Accessed 15 February 2017].

[8] Yao-Jen Chang, Wende Zhang and Tsuhan Chen, "Biometric-Based Cryptographic Key Generation".

[9] Manju Mandot, S.S. Sarangdevot and Sharad Verma, "Fusion Encryption Technique for Finger Print Matching with Text," in *Int'l Journal of Computing, Communications & Instrumentation Engg*, 2016.

[10] Davide Maltoni, Dario Maio, Anil K. Jain and Salil Prabhakar, in *Handbook of Fingerprint Recognition*, Springer, 2009.

[11] Roli Bansal, Priti Sehgal and Punam Bedi, "Minutiae Extraction from Fingerprint Images - a Review," *IJCSI International Journal of Computer Science Issues,* vol. 8, no. 5, 2011.

[12] Zain S. Barham and Dr. Allam Mousa, "Fingerprint Recognition Using Matlab," 2011.

[13] L. O'Gorman, "FINGERPRINT VERIFICATION," Veridicom Inc, Chatham, NJ.

[14] Fengling Han, Jiankun Hu and Xinghuo Yu, "A Biometric Encryption Approach Incorporating Fingerprint Indexing in Key Generation".

[15] Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, "Biometric Template Security," *EURASIP Advances in Signal Processing,* no. Biometrics, 2008.

[16] Aniket Kore, Shiwani Gupta and Kiran Bhandari, "Symmetric Encryption Algorithm Based on Keys Generated from Biometrics," *International Journal of Recent Trends in Engineering & Research* , no. 2455-1457.

[17] B. Raja Rao, Dr. E.V.V.Krishna Rao, S.V.Rama Rao and M. Rama mohan rao, "Finger Print Parameter Based Cryptographic Key Generation," *International Journal of Engineering Research and Applications,* vol. 2, no. 6, pp. 1598-1604, 2012.

[18] Sayani Chandra, . Sayan Paul, Bidyutmala Saha and Sourish Mitra, "Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data over a Network," *IOSR Journal of Computer Engineering* , vol. 12, no. 1, pp. 16-22, 2013.

[19] Ann Cavoukian and Alex Stoianov, "Biometric Encryption Chapter from the Encyclopedia of Biometrics," [Online]. Available: www.ijcaonline.org. [Accessed 20 January 2016].

[20] Ann Cavoukian, Ph.D. and Alex Stoianov, Ph.D., "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy," March 2007. [Online]. Available: www.ipc.on.ca. [Accessed 20 January 2016].

[21] G. C. Kessler, "An Overview of Cryptography," 26 February 2017. [Online]. Available: http://www.garykessler.net/library/crypto.html. [Accessed 1 March 2017].

VITA

Ranjith Jayapal received the Bachelor of Technology in Electrical and Electronics Engineering from the SRM University, Kattankulathur, India, in 2012. He is currently a master student in the College of Computing, Engineering & Construction at University of North Florida, Jacksonville, FL. His research interests include pattern recognition, computer vision and image processing with application in biometrics. He has presented a paper in International Carnahan Conference on Security Technology (ICCST), Orlando, 2016. He is a member of an IEEE-HKN Honor Society, University of North Florida Kappa Nu.